



**Process Control Systems
Industry Conference**

Control System Self Assessment and the Water Sector Roadmap

Candace Chan Sands, PMP

EMA, Inc.

Process Control Systems Industry Conference

La Jolla

August 2008



Outline

- ◆ **Project Background**
- ◆ **DHS CSSP & CS²SAT**
- ◆ **Water Sector Roadmap Strategies**
- ◆ **CS²SAT for Baseline and Benchmarking – A Demo**
- ◆ **Regional Workshops & Training Plans**
- ◆ **Next Steps**
- ◆ **Q&A**
- ◆ **Case Studies – JEA and Broward County**

PROJECT BACKGROUND

- ◆ Many infrastructure security initiatives underway prior to 2001
- ◆ U.S. EPA Water Security Division – supports a spectrum of security projects
- ◆ WERF awarded EPA grant in '02 - created several projects including *Project: Security Measures for Computerized and Automated Systems at W/WW Facilities*.
- ◆ AwwaRF (WRF) joined the research sponsor team in Jan 04 - scope expanded to also include water facilities
- ◆ Research project started 9/2004
- ◆ Joined DHS/CSSP in 9/2005

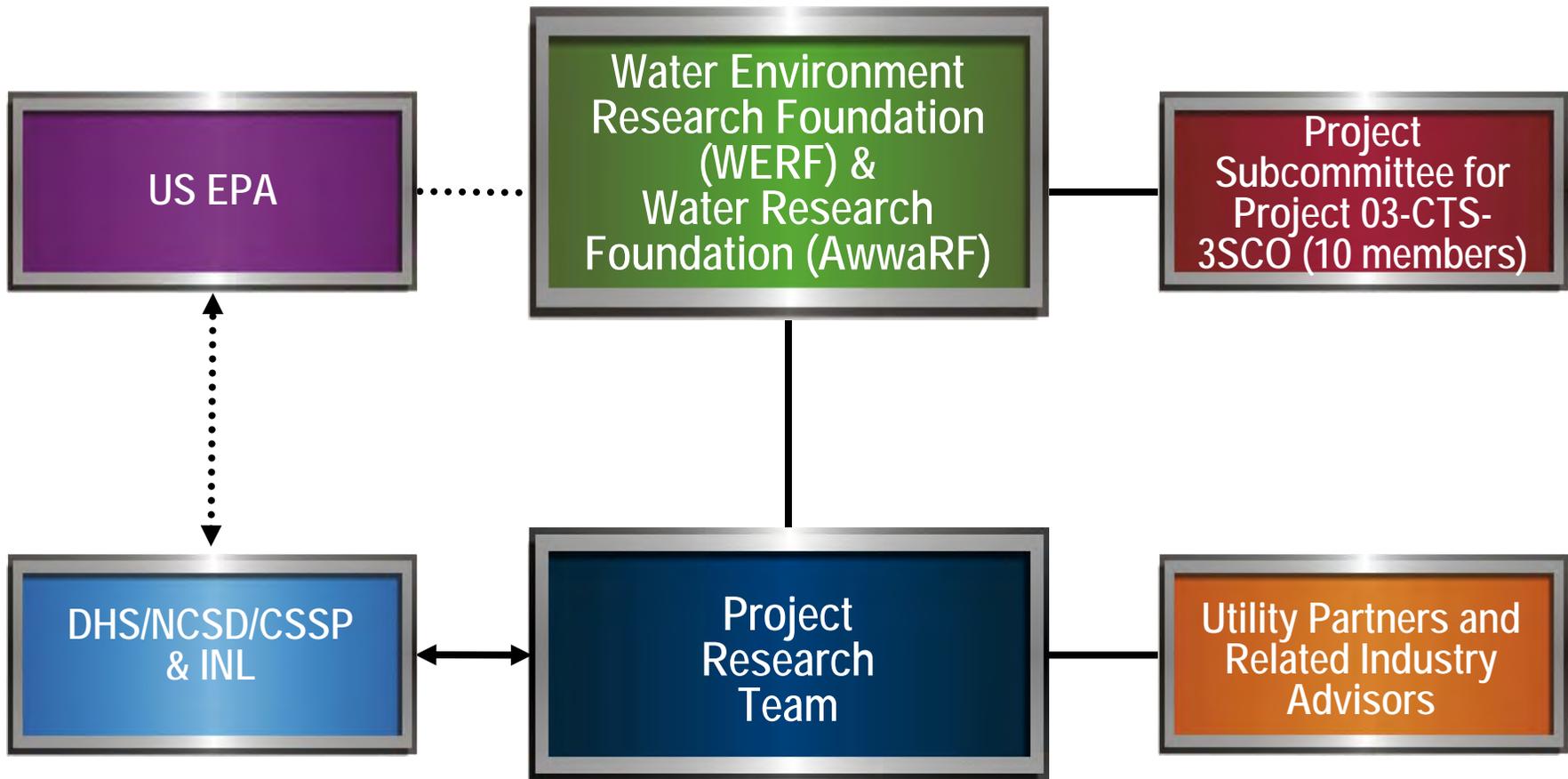
PROJECT BACKGROUND - RESEARCH OBJECTIVES

“The material & tools produced that will provide the necessary guidance to utilities on how to secure and protect computerized and automated systems. This project also will document technology currently available (and being further developed) to sense and correct such security breaches and alert relevant authorities...”

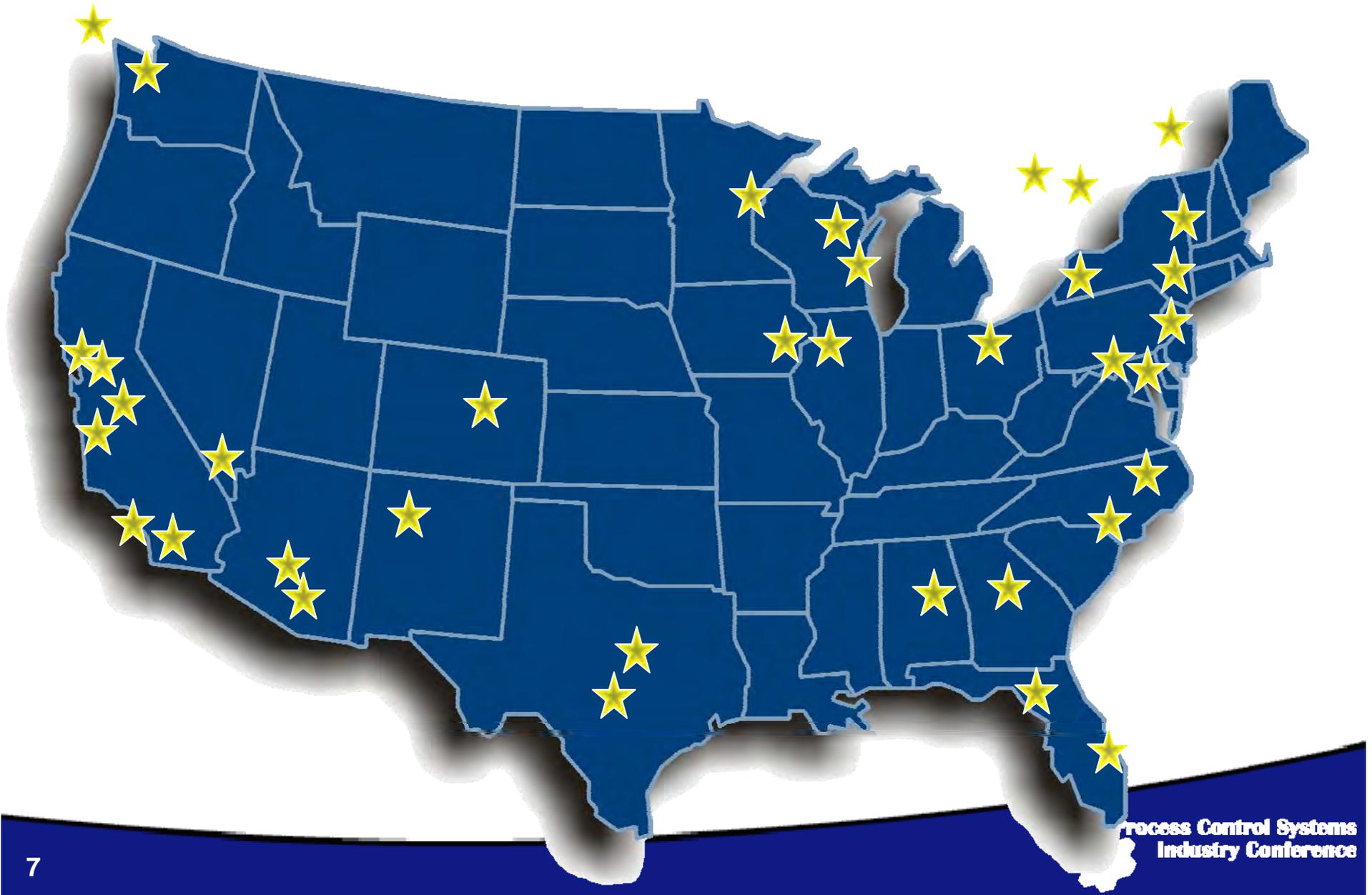
PROJECT BACKGROUND - PRODUCTS

- ◆ Resources based on standards and results – i.e., NIST PCSRF guidance and specifications, ISA standards, leading practices, trends, and progress in other related industries
- ◆ Leading Practices and Guidance
- ◆ Lessons Learned from Pilots and Beta Testing
- ◆ Self-assessment methodology documentation (e.g., User's Guide)
- ◆ An “expert system” software tool: CS SESAT, DHS/CSSP CS²SAT

PROJECT TEAM



UTILITY PARTNERS & TESTERS



CONNECTION BETWEEN EPA SECURITY PROJECTS & DHS

- *National Strategy to Secure Cyberspace, Feb 2003*
- *Department of Homeland Security → Cyberspace Security*
- *Critical Infrastructure Lead Agencies identified - US EPA lead agency for Water Sector*
- *INL lead in CSSP/Cs2SAT development*

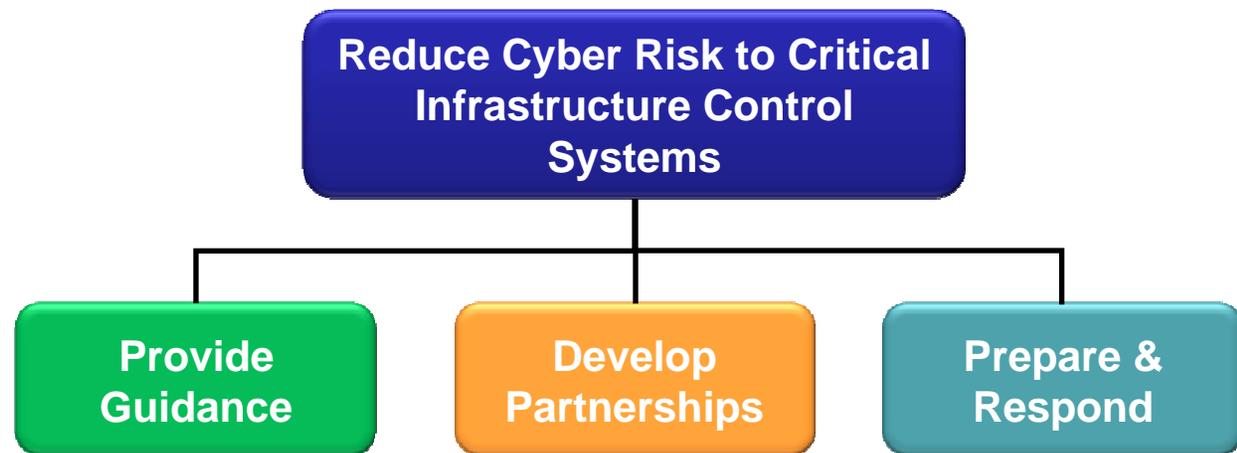
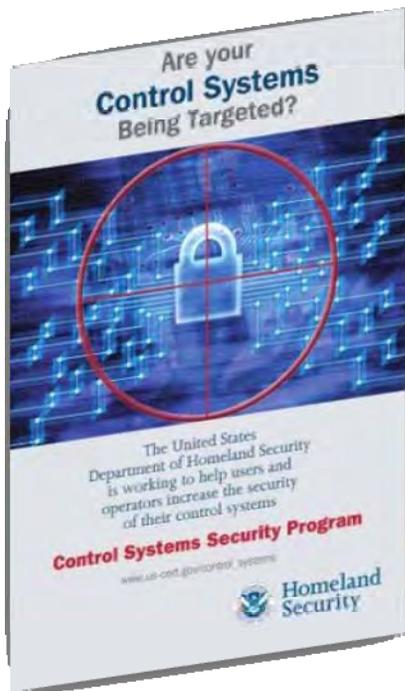
COLLABORATION BENEFITS

- Brought together knowledge and experience: Customizations based on our work with WERF CS SESAT
- A more robust self assessment tool
- Eliminates dup of effort (or conflicts)
- Model collaborative effort → water sector Beta Tested by Utilities/Operators
- More Bang-for-the Buck: Leveraging a National Program (DHS CSSP)

DHS National Cyber Security Division

Control Systems Security Program

Reduce Cyber Risk to Critical Infrastructure Control Systems by Providing Guidance, Building Partnerships & Preparing to Respond to Incidents”

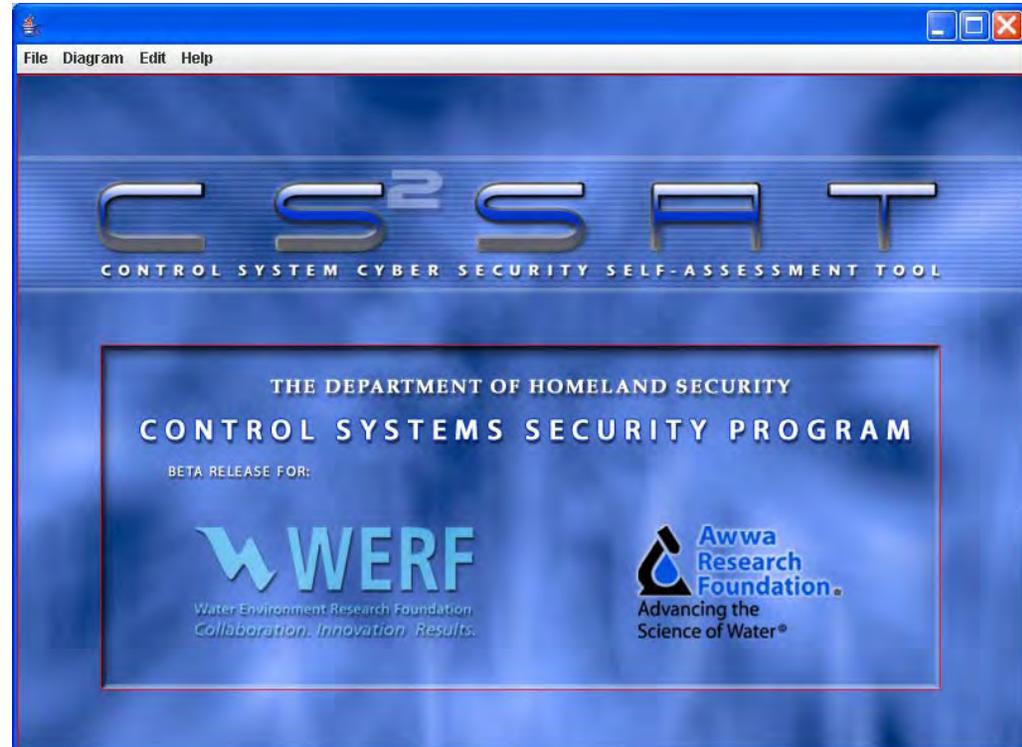


DHS National Cyber Security Division

Control Systems Security Program

Provide
Guidance

Prepare &
Respond



SECTOR EXPERIENCE WITH SELF ASSESSMENT TOOLS

- ◆ **WERF/AwwaRF CS SESAT - 2004/2005**

- Beta Tested with 8 Utility Partners
- Conducted 3 Site Assessments

- ◆ **DHS/CSSP CS2SAT V1.0-1.8 (2006/07)**

- Customization for Water
- Beta Test 1 included 6 Utility Partners
- Conducted 2 Site Assessments
- Beta Test 2 involved PSC members, Utility Partners, and over 50 Utilities/SMEs

- ◆ **Received substantial feedback/comments from Sector – US and Canada**

Where Are We?

General Release Rollout (9/2008)

Version 2 release and validation (Aug/Sept 08)

Tool Enhancement/Refinement (Aug-Sept 07)

Outreach and Demos (Mar-Oct 07)

Beta Test – Phase 2 (Mar-Jul 07)

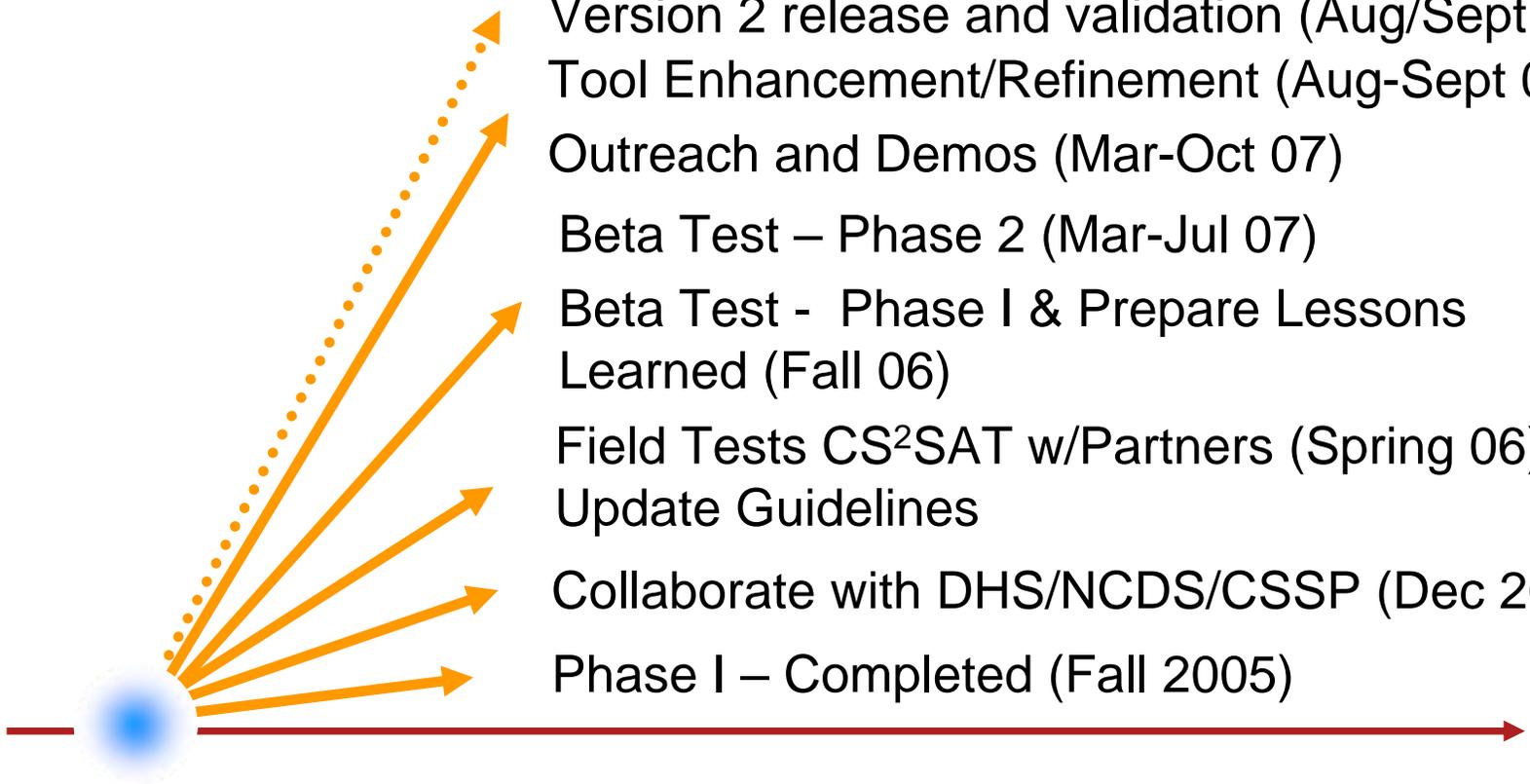
Beta Test - Phase I & Prepare Lessons Learned (Fall 06)

Field Tests CS²SAT w/Partners (Spring 06)

Update Guidelines

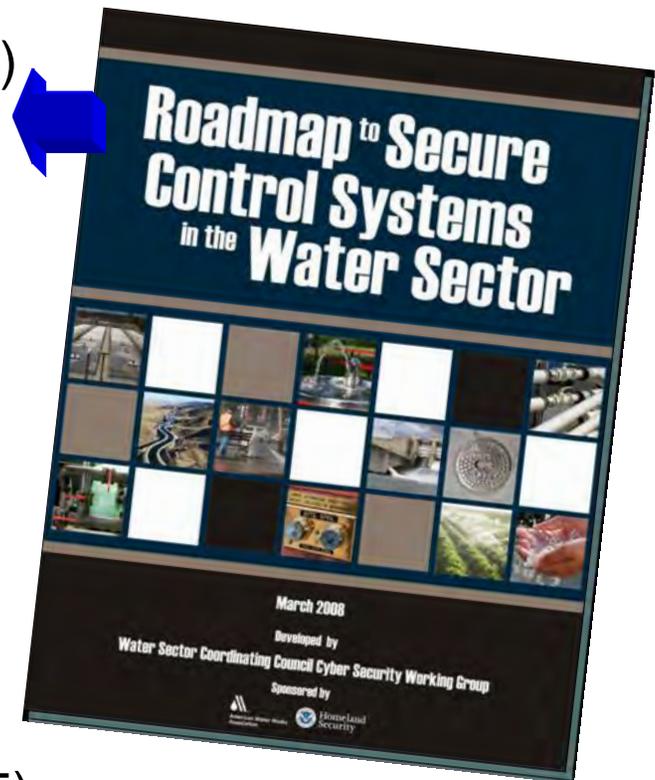
Collaborate with DHS/NCDS/CSSP (Dec 2005)

Phase I – Completed (Fall 2005)

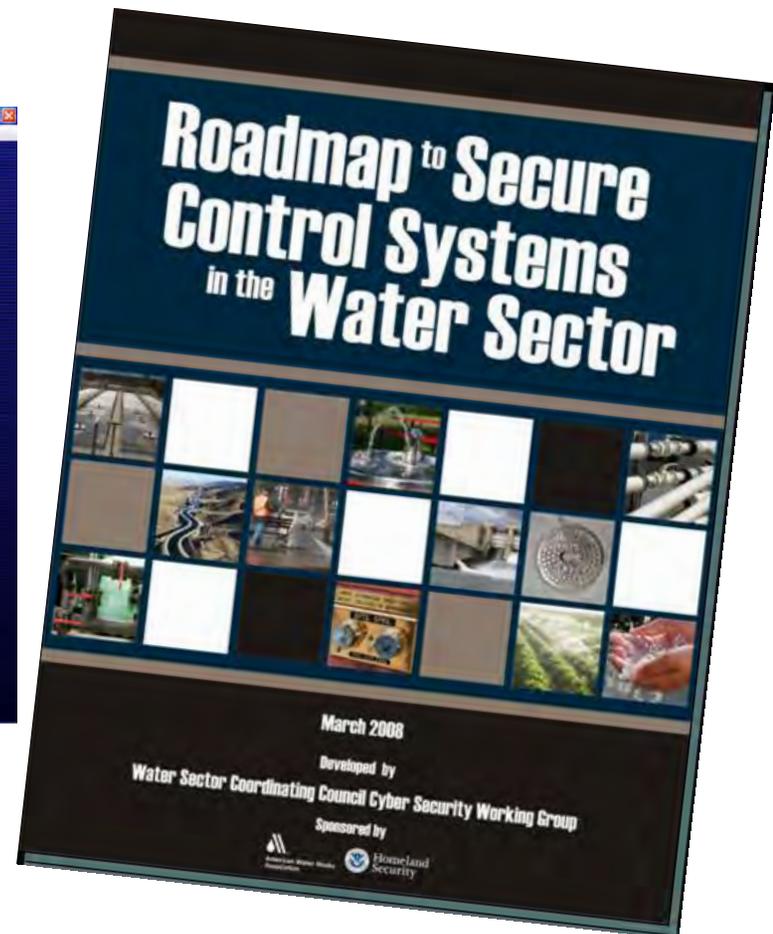
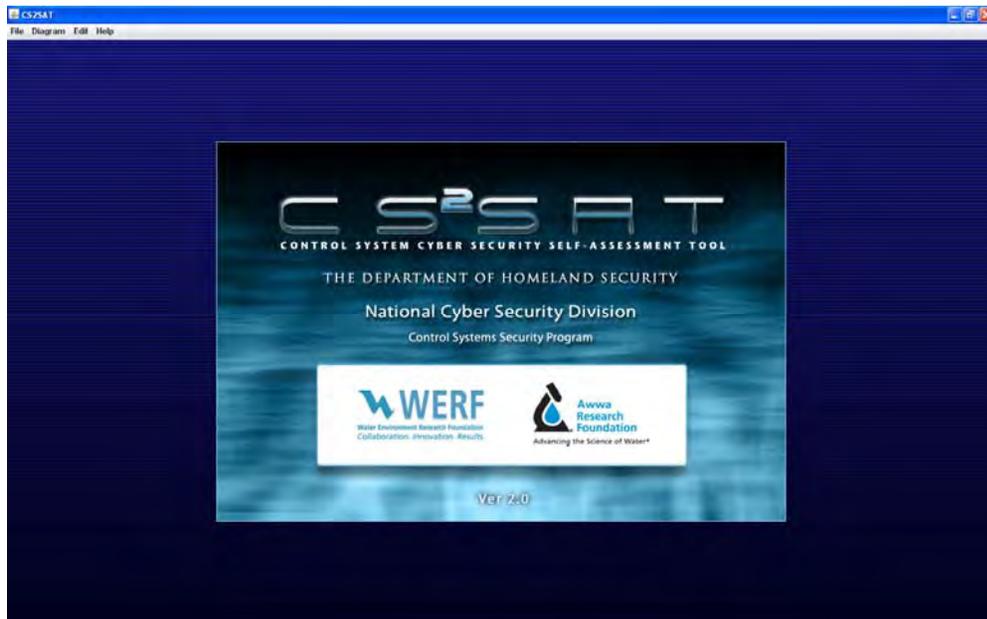


Where Are We?

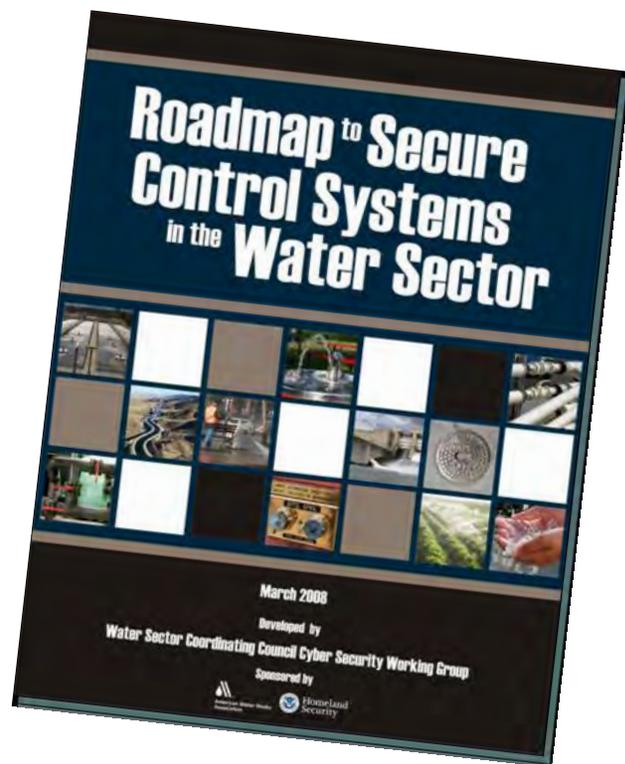
- General Release Rollout (9/2008)
- Version 2 release and validation (Aug/Sept 08)
- Tool Enhancement/Refinement (Aug-Sept 07)
- Outreach and Demos (Mar-Oct 07)
- Beta Test – Phase 2 (Mar-Jul 07)
- Beta Test - Phase I & Prepare Lessons Learned (Fall 06)
- Field Tests CS²SAT w/Partners (Spring 06)
- Update Guidelines
- Collaborate with DHS/NCDS/CSSP (Dec 2005)
- Phase I – Completed (Fall 2005)



CS²SAT & THE WATER SECTOR



WATER SECTOR ROADMAP



- Development started in September 2007
- Approved in March 2008
- Involved 30 W/WW executives from 23 orgs including DHS & EPA
- Sets the stage for the next 10 yrs

ROADMAP STRATEGIES

Four main categories:

- ◆ **Develop and deploy ICS security programs**
- ◆ **Assess risk**
- ◆ **Develop and implement risk mitigation measures**
- ◆ **Promote partnership and continue outreach**

CS²SAT & ROADMAP STRATEGIES

- ◆ Develop and deploy ICS security programs

- ◆ Assess risk

- ◆ Develop and implement risk mitigation measures



ASSESS RISK – USING CS²SAT

- **Train the Trainers/Power Users on CS2SAT (Self Assessment Tool)** - Provide ongoing training, through collaboration with WERF/AwwaRF CS2SAT project.
- **Use CS2SAT tool for baselining and measuring progress** -measure cyber security preparedness using the self assessment tool. Establish a baseline measurement.
- **Analyze and collate progress** - further analysis and progress measurement, as well as benchmarking to other utility partners will take place.

ASSESS RISK – USING CS²SAT



WHAT IS CS²SAT?



“...a desktop software tool which guides users through a step-by-step process to collect facility specific control system information and then makes appropriate recommendations for improving the system’s cyber security posture.”

BASIS OF THE CS²SAT

Requirements Derived from Widely Recognized Standards

NIST System Protection Profile, Critical Infrastructure Process Control Systems (SPP-CIPCS), Rev. 1.07 (Draft)

NIST SPP Industrial Control Systems (SPP-ICS), Rev. 1.0

Common Criteria ISO/IEC 15408 Versions 2.1 to 3.1

**NIST Special Publication 800-53
(Recommended Security Controls for Federal Information Systems) Rev. 0**

**NERC Critical Infrastructure Protection (CIP)
Reliability Standards CIP-002 – CIP-009**

**DoD Instruction 8500.2
Information Assurance Implementation, February 6, 2003**

CS²SAT CAPABILITIES

What the CS²SAT CAN do:



- Provides user a stand alone, interactive cyber security assessment tool
- Provides a consistent means of evaluating a control system network as part of a comprehensive security assessment
- Provides specific security recommendations
- Provides standards based information & reports
- Provides a baseline of security posture

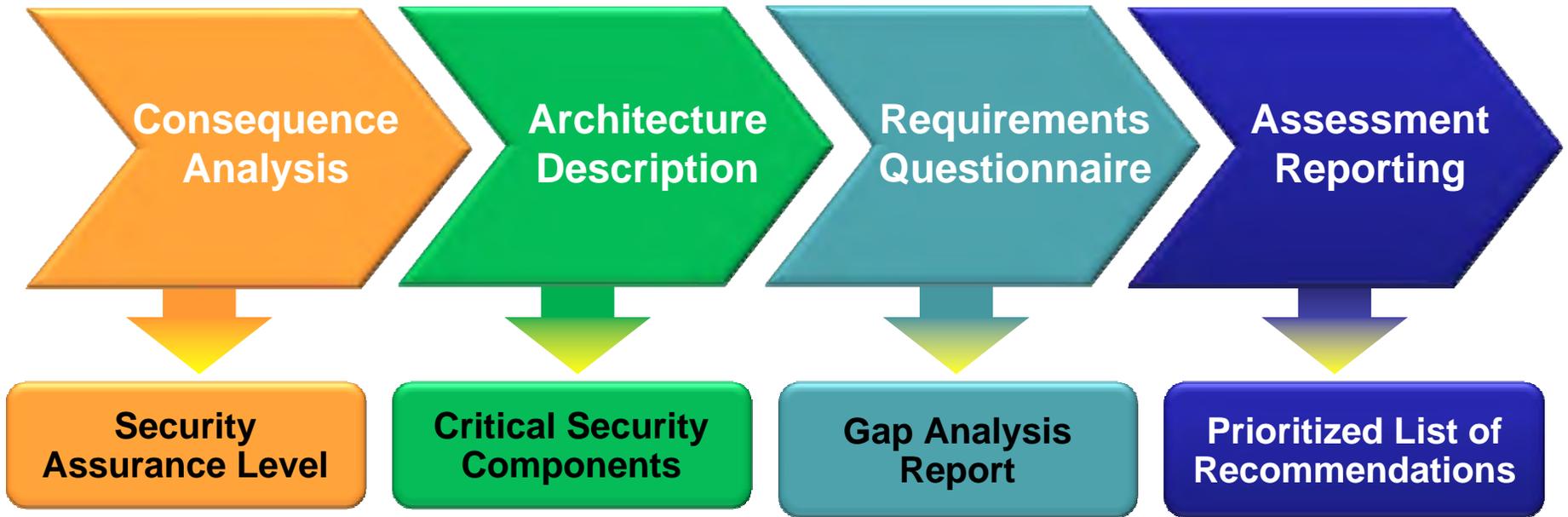
What the CS²SAT does NOT do:



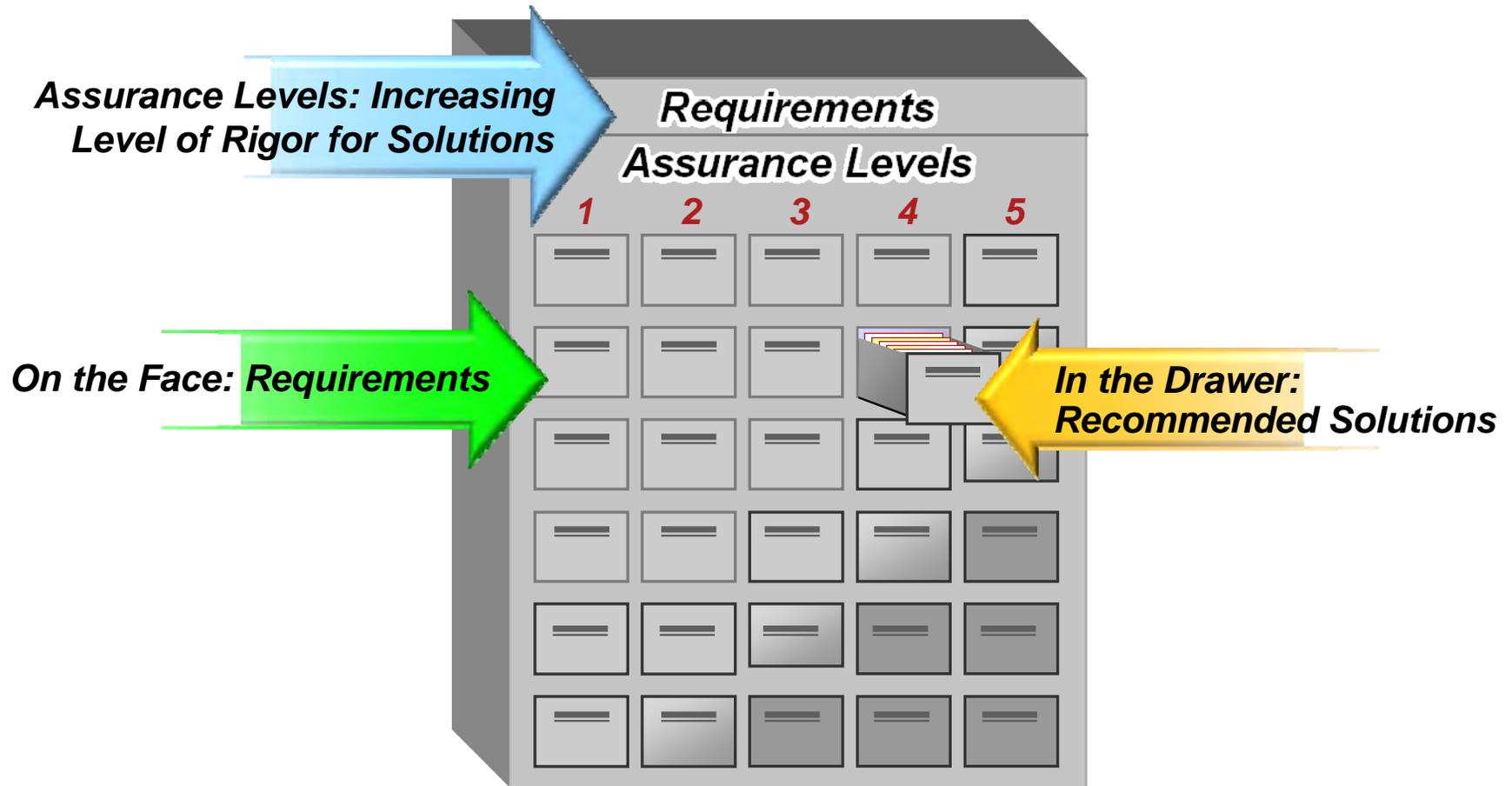
- Ensure that the answers provided are correct
- Ensure that individuals are complying with current security policy & procedures
- Ensure that security enhancements are implemented correctly

CS²SAT FLOW PROCESS

Four Independent Elements

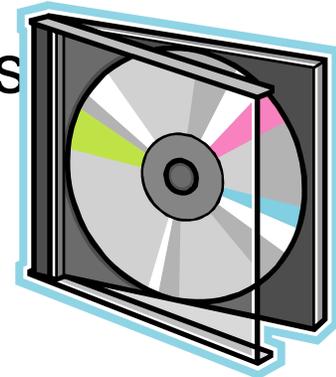


DRAW FROM DATABASE OF SOLUTIONS

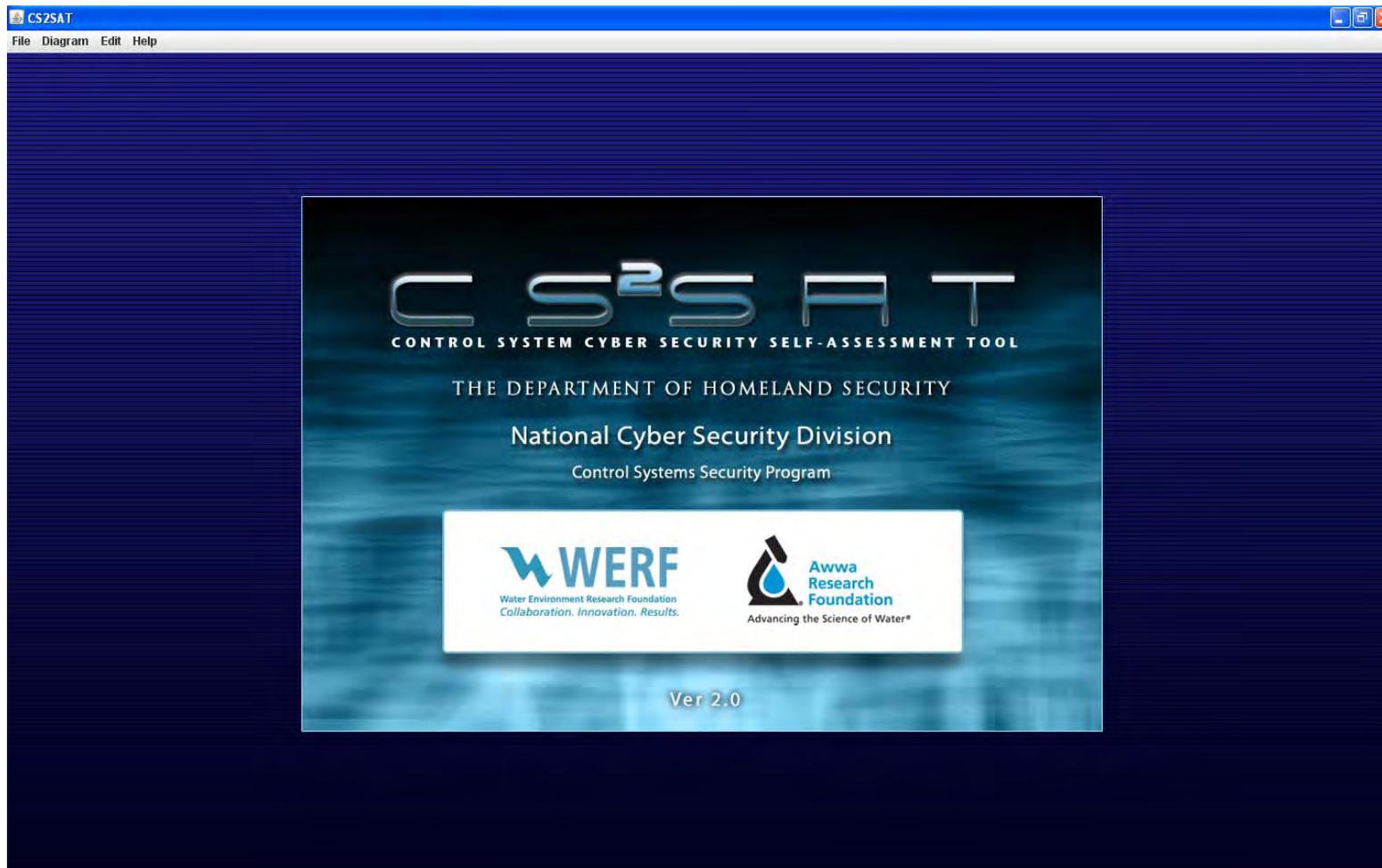


SYSTEM REQUIREMENTS – CS²SAT Ver 2

- 500 MHz Intel/IBM Compatible) processor
- CD- ROM Drive (CD Version)
- 700 MB of free Hard Disk Space
- 512 MB of Memory
- Microsoft Windows XP
- Adobe Acrobat Reader 8.0 or later
- Java Runtime Environment Version 5.0 release 11



BASELINE & BENCHMARKS – A DEMO



INTERPRETING THE RESULTS

◆ On Screen Report

- Gap Analysis
- Recommendations or Solutions
- Requirement Source Information

◆ Hard Copy Report

- Bar Chart Summary
- Pie Chart Summary
- Gap Analysis
- Sorted Gap Analysis (Prioritized list)
- Standard Specific Report (NERC CIP comparison)
- Response Summary



ON-LINE & HARDCOPY REPORTS

The screenshot displays the CS2SAT Annual Assessment 08-08 software interface. The main window shows a list of 17 questions under the 'Layer: Admin' and 'Component: Administrative' sections. The 'Security Assurance Level' is set to 5 and the 'ISO/IEC Rev. 3.1' is selected. A 'Print Dialog' box is open, allowing for sub-report selection. The dialog includes checkboxes for 'Assessment Information', 'Summary', and 'SAL Questions and Answers'. It also features 'ISO/IEC Rev. 3.1' and 'Component' sections, each with a 'Level Selection' dropdown set to 5 and a 'Gap Analysis' checkbox. The 'Page Footer Text' field contains 'summary report'. 'Print' and 'Cancel' buttons are at the bottom of the dialog.

CS2SAT - Annual Assessment 08-08

File Diagram Edit Help

Assessment Info Navigation SAL Questions ISO/IEC 3.1 Component Diagram Components Assessment Report Document Library

Security Assurance Level: 5 ISO/IEC Rev. 3.1

Layer: Admin

Component: Administrative

Question: 1. Is the control system appropriately labeled with a unique label that is also used consistently in all documentation, such as network schematics, drawings, diagrams, procedures, user manuals, maintenance documentation, operator documentation, and other media?

Question: 2. Does the configuration management plan or similar documentation describe a method of unique identification of configuration items?

Question: 3. Are changes to configuration items limited to those changes formally authorized per a configuration management plan? Select one of the following that best describes your configuration management implementation.

Question: 4. Which of the following best describes acceptance procedures for changes to the control system and related IT supporting systems?

Question: 5. Are advanced support procedures and methods including event logs, independence of design, tools for discovery of impacted configuration items, and other advanced configuration management methods and tools (including Automated Software) used to support design, development, review, and approval?

Question: 6. Is the evaluation evidence (hazards analysis, safety analysis, etc.) used in the change process (i.e., control system and supporting IT infrastructure changes) included in the configuration list?

Question: 7. Is the vendor/developer of security-related configuration items identified on the configuration list?

Question: 8. Is the implementation representation (see HELP) included in the configuration list and subject to configuration management requirements?

Question: 9. Are control system security flaws maintained on the configuration list for tracking to resolution?

Question: 10. Are operational and/or development tools maintained on the configuration list to ensure modifications are made as necessary to these tools and flaws are traceable to solutions/patches?

Question: 11. Does delivery documentation describe all procedures that are necessary to maintain security when distributing versions of the system to the user?

Question: 12. Is development security supported with documentation that describes vendor/developer security measures including physical, procedural, personnel and other security measures necessary to protect confidentiality and integrity of design and implementation of hardware/software/firmware in the development environment?

Question: 13. Does the developer documentation provide evidence of the necessary level of protection to maintain confidentiality and integrity of the system during development?

Question: 14. Has the vendor/developer provided flaw remediation procedures for the control system software/hardware/firmware?

Question: 15. Has the vendor/developer documented the flaw reporting procedures and provided documentation on installation with assurance that no new flaws are introduced as a result of the corrections?

Question: 16. Do flaw remediation procedures include timely response for distribution of security flaw reports and points of contact for all reports and enquiries?

Question: 17. Does the user documentation describe implementation and use of role-based access controls and the accessible functions?

Print Dialog

Sub-Report Selection:

Assessment Information

Summary

SAL Questions and Answers

ISO/IEC Rev. 3.1

5 Level Selection

Gap Analysis

Component

5 Level Selection

Gap Analysis

Top 20 Gap Analysis for Components

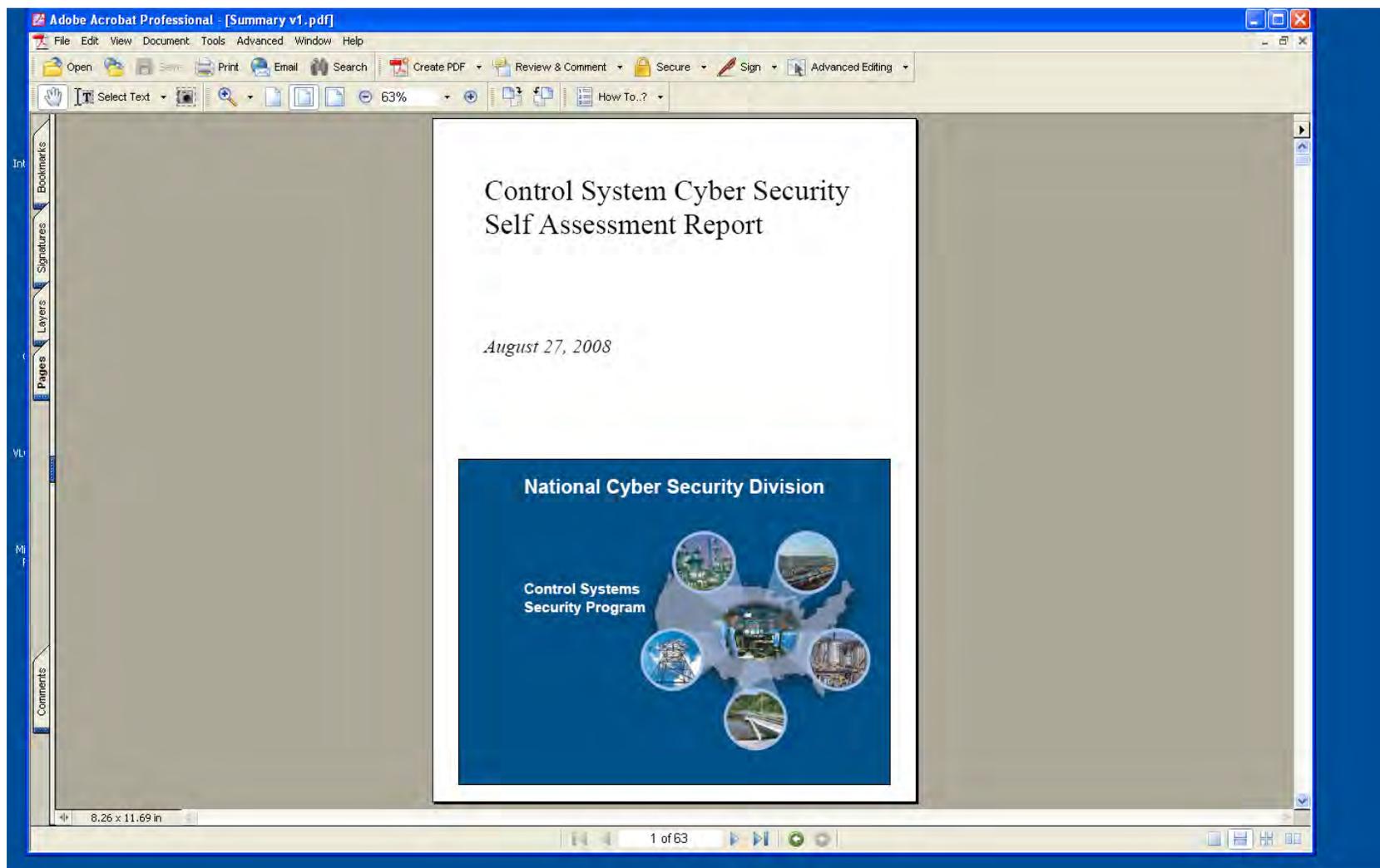
Questions and Answers

Page Footer Text

summary report

Print Cancel

SAMPLE REPORTS



NEXT STEPS

- WATER SECTOR ONLY -

- Roadmap Implementation
- CS²SAT Water Sector Outreach / Distribution: a multi-prong approach
- Version 2 available to users mid Sept 08
- Provide information and training
- Collect feedback and experience

HOW TO GET A COPY OF CS²SAT (ver. 2)

WATER SECTOR ONLY -

- **WERF OR AwwaRF/WRF members**
 - Non-members must purchase tool thru licensed orgs
- **Submit request to WERF or AwwaRF**
- **Distribution mid-Sept 08**
- **Attend intro session (WebEx) or a training workshop**
- **Agree to End User Licensing Agreement Terms**
- **Use the tool**
- **Join User Group & provide feedback**

CCS6

PLANNED INTRO & TRAINING SESSIONS

WebEx Sessions (~50 mins):

October 2008

November 2008

Tentative training workshops – Train the Trainers (~3 hrs):

December 2008

February 2009

April 2009

Webpage for training info: werf.org/cs2sat (Avail Sept 09)

Slide 33

CCS6

The scxheduled is to be confirmed. There may be other venues. need to check with INL.

Candace Chan-Sands, 7/24/2008

QUESTIONS?

CONTACT INFORMATION

Candace Sands, PMP

Program Manager

EMA, Inc.

csands@ema-inc.com

520.975.9758 cell

215.792.7510 office

WERF Contact:

Dr. Roy Ramani

Program Director

rramani@werf.org

(703) 684-2470 x7912 office

WRF Contact:

Robert C. Renner, D.E.,P.E.E.

Executive Director

(303) 347-6150 office